

03/01/00  
Jc677 U.S. PTO

103-07-00

A

UTILITY PATENT APPLICATION TRANSMITTAL

(New Nonprovisional Applications Under 37 CFR § 1.53(b))

Attorney Docket No.

1018.072US1

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Transmitted herewith is the patent application of ( ) application identifier or (X) first named inventor, Neta Amit, entitled Secured Distributed Impersonation, for a(n):

(X) Original Patent Application.

( ) Continuing Application (prior application not abandoned):

( ) Continuation ( ) Divisional ( ) Continuation-in-part (CIP)

of prior application No: \_\_\_\_\_ Filed on: \_\_\_\_\_

( ) A statement claiming priority under 35 USC § 120 has been added to the specification.

Enclosed are:

(X) Specification; 23 Total Pages.

(X) Drawing(s); 3 Total Sheets.

(X) Oath or Declaration:

(X) A Newly Executed Combined Declaration and Power of Attorney:

( ) Signed. (X) Unsigned. ( ) Partially Signed.

( ) A Copy from a Prior Application for Continuation/Divisional (37 CFR § 1.63(d)).

( ) Incorporation by Reference. The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered as being part of the disclosure of the accompanying application and is hereby incorporated herein by reference.

( ) Signed Statement Deleting Inventor(s) Named in the Prior Application. (37 CFR § 163(d)(2)).

( ) Power of Attorney.

(X) Return Receipt Postcard.

( ) Associate Power of Attorney.

( ) A Check in the amount of \$ \_\_\_\_\_ for the Filing Fee.

( ) Preliminary Amendment.

( ) Information Disclosure Statement and Form PTO-1449.

( ) A Duplicate Copy of this Form for Processing Fee Against Deposit Account.

( ) A Certified Copy of Priority Documents (if foreign priority is claimed).

( ) Statement(s) of Status as a Small Entity.

( ) Statement(s) of Status as a Small Entity Filed in Prior Application, Status Still Proper and Desired.

(X) Patent application data entry format sheets for OCR.

CLAIMS AS FILED				
FOR	NO. FILED	NO. EXTRA	RATE	FEE
Total Claims	21	1	\$18.00	\$ 18.00
Independent Claims	3	0	\$78.00	\$ 0.00
Multiple Dependent Claims (if applicable)				\$0.00
Assignment Recording Fee				\$0.00
Basic Filing Fee				\$690.00
Total Filing Fee				\$ 708.00

Charge \$ \_\_\_\_\_ to Deposit Account \_\_\_\_\_ pursuant to 37 CFR § 1.25. At any time during the pendency of this application, please charge any fees required or credit any overpayment to this Deposit Account.

Respectfully submitted,

By:

Michael A. Dryja, Attorney of Record, Reg. No. 39662

Date: 3/1/2000

Correspondence Address:

Law Offices of Michael Dryja  
704 228th Avenue NE PMB 694  
Redmond, WA 98053  
Phone: 425-427-5094  
Fax: 206-374-2819



23441

PATENT TRADEMARK OFFICE

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to addressee" service under 37 CFR § 1.10 in an envelope addressed to The Assistant Commissioner for Patents, Washington, DC 20231, on Mar 1, 2000, by Michael Dryja, and having "express mail" mailing label no. EK530297201US.

Signature of Michael Dryja

Jc678 U.S. PTO  
09/516402  
03/01/00

#### Inventor Information

Inventor One Given Name:: Neta  
Family Name:: Amit  
Postal Address Line One:: 33 Yotam Street  
City:: Haifa  
Postal or Zip Code:: 34675  
Country:: Israel  
Citizenship Country:: Israeli

Inventor Two Given Name:: Alexander  
Family Name:: Frank  
Postal Address Line One:: 11 Mizpe St.  
City:: Ramat-Gan  
Postal or Zip Code:: 52493  
Country:: Israel  
Citizenship Country:: Israeli, German

#### Correspondence Information

Correspondence Customer Number:: 23441  
Telephone:: (425) 427-5094  
Fax:: (206) 374-2819  
Electronic Mail One:: mike@dryjapat.com  
Electronic Mail Two:: sherry@dryja.com

#### Application Information

Title Line One:: Secured Distributed  
Title Line Two:: Impersonation  
Total Drawing Sheets:: 3  
Formal Drawings?:: Yes  
Application Type:: Utility  
Docket Number:: 1018.072US1

#### Representative Information

Registration Number One:: 39,662  
Registration Number Two:: 32,628  
Registration Number Three:: 32,022

# SECURED DISTRIBUTED IMPERSONATION

## FIELD OF THE INVENTION

This invention relates generally to batch systems, such as message transaction batch systems, and more particularly to secured distributed impersonation within such systems.

## BACKGROUND OF THE INVENTION

When organizations need to have large-scale computer systems that hold mission critical information, such as purchase orders, financial information, etc., they usually resort to message transaction systems. Message transaction systems ensure that data is not lost if the system crashes, and also that data is not duplicated – such as ensuring that two copies of the same purchase order are not processed, etc. A transaction is an activity or a request, such as an order, a purchase, a change, or an addition to a database of information. Transactions usually update one or more files on a non-volatile storage such as a hard disk drive, and thus can serve as both an audit trail and a history for future analyses. A transaction can include one or more messages. A transaction is considered committed when all the messages of the transaction have been received and processed.

Message transaction systems can be batch systems. A batch is a set of requests that are processed together, often long after the requests have been submitted. For example, batch systems can execute the batches during non-peak periods, such as overnight, when usually requests are not being received as frequently. Typically, each batch is a sequence of transactions, and is executed sequentially, one transaction at a time. A batch system in the context of a message transaction system can be an off-line

system, where transactions are collected throughout the day, for example, and then processed at night.

Batch systems can run in secure distributed environments, where there can be literally thousands of computers over which the batch “jobs” (viz., units of work running on the computer) are executed. Frequently, each computer has only limited access rights within the system, and usually does not have global rights to the entire system. This is problematic because a given computer which is given a particular transaction to commit (e.g., a particular batch job to execute) may not have all the access rights necessary to execute the job. That is, the dispatch computer, which is responsible for parceling out transactions for performance by the computers within the system, generally gives transactions to the computers as they become available, so that the computing resources within the system are leveraged. But the dispatch computer may parcel a job out to a computer that does not have adequate access privileges to execute the job.

Within the prior art, there are different ways to solve this problem, all of which are disadvantageous. First, a technician with sufficient privileges can manually start all the computers – that is, log onto all the computers – before the batch processing starts, such that all the computers are “live,” and therefore all resources are open and available to every computer. However, this is not practical, and can also pose a security risk, inasmuch as when the processing takes place, the system becomes completely open and thus insecure.

Second, passwords for various accounts can be stored locally on the computers. Thus, when a computer needs access to a resource that it does not have privileges for, the computer can use the passwords it has at its disposal to properly access the resource.

This, too, however, is a security risk, since a hacker breaking into the system may be able to obtain all the passwords for the entire system from a single compromised computer. Furthermore, there is a maintenance problem with this approach – passwords frequently change, such that the password stores throughout the system must be updated.

5 For these and other reasons, therefore, there is a need for the present invention.

## SUMMARY OF THE INVENTION

The invention relates to secured distributed impersonation, such as can be used within batch systems, such as batch message transaction systems. In one embodiment, a method includes sending a request for network account credentials from an originating  
10 account associated with an unpublished object to a dispatch associated with a published object. In one embodiment, both the unpublished and the published objects can each be a message queue. The request is sent specifically to the published object, and identifies the unpublished object. The originating account can be at a local computer, for example, within a system of which the dispatch is also a part. The network account credentials can  
15 be, for example, the account credentials that the originating account needs to properly perform a job that has been assigned to it.

The dispatch authenticates the originating account. Upon successful authentication, the network account credentials are sent to the originating account. In one embodiment, these account credentials are included in data that is generically referred to  
20 herein in a non-restrictive and non-limited manner as an emblem, which can in one embodiment be a secure manner by which the credentials are transmitted. For example, the emblem can be a token, as known within the art. The emblem is specifically sent to the unpublished object associated within the originating account, as identified in the



## BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagram of an operating environment in conjunction with which embodiments of the invention can be practiced;

FIG. 2 is a diagram of a system according to an embodiment of the invention;

5 and,

FIG. 3 is a flowchart of a method according to an embodiment of the invention.

## DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of exemplary embodiments of the invention, reference is made to the accompanying drawings, which form a part hereof, and in which  
10 is shown by way of illustration specific exemplary embodiments in which the invention may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that logical, mechanical, electrical and other changes may be made without departing from the spirit or scope of the present invention. The  
15 following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims.

Some portions of the detailed descriptions that follow are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those  
20 skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these

quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like. It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that throughout the present invention, discussions utilizing terms such as processing or computing or calculating or determining or displaying or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

## Operating Environment

Referring to FIG. 1, a diagram of the hardware and operating environment in conjunction with which embodiments of the invention may be practiced is shown. The description of FIG. 1 is intended to provide a brief, general description of suitable computer hardware and a suitable computing environment in conjunction with which the invention may be implemented. Although not required, the invention is described in the general context of computer-executable instructions, such as program modules, being executed by a computer, such as a personal computer. Generally, program modules

include routines, programs, objects, components, data structures, etc., that perform particular tasks or implement particular abstract data types.

Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multiprocessor systems, microprocessor-based or programmable consumer electronics, network PC's, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

The exemplary hardware and operating environment of FIG. 1 for implementing the invention includes a general-purpose computing-device in the form of a computer, including a processing unit 21, a system memory 22, and a system bus 23 that operatively couples various system components including the system memory to the processing unit 21. There may be only one or there may be more than one processing unit 21, such that the processor of computer comprises a single central-processing unit (CPU), or a plurality of processing units, commonly referred to as a parallel processing environment. The computer may be a conventional computer, a distributed computer, or any other type of computer; the invention is not so limited.

The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory may also be referred to as simply the memory, and includes read only memory (ROM) 24 and random access memory (RAM).

A basic input/output system (BIOS) 26, containing the basic routines that help to transfer information between elements within the computer, such as during start-up, is stored in ROM 24. The computer further includes a hard disk drive 27 for reading from and writing to a hard disk, not shown, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to a removable optical disk 31 such as a CD ROM or other optical media.

The hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive interface 33, and an optical disk drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer-readable instructions, data structures, program modules and other data for the computer. It should be appreciated by those skilled in the art that any type of computer-readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read only memories (ROMs), and the like, may be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24, or RAM, including an operating system 35, one or more application programs 36, other program modules 37, and program data 38. A user may enter commands and information into the personal computer through input devices such as a keyboard 40 and pointing device 42. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46

that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port, or a universal serial bus (USB). A monitor 47 or other type of display device is also connected to the system bus 23 via an interface, such as a video adapter 48. In addition to the monitor, computers typically include other peripheral  
5 output devices (not shown), such as speakers and printers.

The computer may operate in a networked environment using logical connections to one or more remote computers, such as remote computer 49. These logical connections are achieved by a communication device coupled to or a part of the computer; the invention is not limited to a particular type of communications device. The  
10 remote computer 49 may be another computer, a server, a router, a network PC, a client, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer, although only a memory storage device has been illustrated in FIG. 1. The logical connections depicted in FIG. 1 include a local-area network (LAN) 51 and a wide-area network (WAN) 52. Such networking  
15 environments are commonplace in office networks, enterprise-wide computer networks, intranets and the Internet, which are all types of networks.

When used in a LAN-networking environment, the computer is connected to the local network 51 through a network interface or adapter 53, which is one type of communications device. When used in a WAN-networking environment, the computer  
20 typically includes a modem 54, a type of communications device, or any other type of communications device for establishing communications over the wide area network 52, such as the Internet. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program

modules depicted relative to the personal computer, or portions thereof, may be stored in the remote memory storage device. It is appreciated that the network connections shown are exemplary and other means of and communications devices for establishing a communications link between the computers may be used.

## 5 Systems

In this section of the detailed description, systems according to varying embodiments of the invention are described. The systems are described in conjunction with FIG. 2, which is a diagram of a system according to an embodiment of the invention. The system can in one embodiment be a batch system, such as a batch  
10 message transaction system, although the invention is not so limited, as can be appreciated by those of ordinary skill within the art.

Referring now to FIG. 2, the system 200 includes a dispatch 201, a first originator 202, a second originator 204, and an agent 206. Each of these can in one embodiment be a computer, such as that described in the preceding section of the detailed description.

15 Alternatively, each of these can be a separate software program, or a separate task and/or thread, running on one or more computers. The invention is not so limited.

Each of the originators 202 and 204, as well as the agent 206, can in one embodiment be likened to and/or have a corresponding account. An account generally, non-restrictively, and in a non-limited manner refers to herein as an established  
20 relationship between a user and a computer, network or information service. Such accounts can include network accounts, local accounts, and machine accounts, as can be appreciated by those of ordinary skill within the art. For example, local accounts can include user accounts, such as administrator accounts, user accounts, guest accounts, etc.

Gaining access to such accounts may require a username and password, and each account has a set of permissions as to the resources it is able to access. In general, as can be appreciated by those of ordinary skill within the art, each account has an identification (ID) corresponding to the owner.

5           For the system 200 of FIG. 2, there typically is more than three network accounts and/or computers, however, only three are specifically shown for illustrative clarity purposes. The dispatch 201 also has a corresponding account, which is referred to as the batch account herein. The accounts for the originators 202 and 204 are referred to as originating accounts, while the account for the agent 206 is referred to as the agent  
10   account. At least the batch account for the dispatch 201, and the agent account for the agent 206, are network accounts, which means that they have privileges to resources across the network. The credentials for any account refer to, in a non-restrictive and a non-limited manner, the identifying information that enables the account to have its access privileges. For example, the credentials for a network account allow the network  
15   account its privileges to access resources across the network, in some defined manner.

          The agent account 206, is capable of being proxy logged onto, and of being remototed to another account. Proxy logon refers to the process by which a first account logs onto a second account in a secured manner without having to present a secret identifier which belongs to the second account, such as a password. Remoting refers to  
20   the transfer of a first account to a second account, such that the second account is able to use the first account and its permissions as if it were the first account. (Accounts are transferred in one embodiment by transfer of their credentials.)

The dispatch 201 generally determines what pending tasks and/or jobs should be done next and assigns the available resources, such as the originators 202 and 204, and the agent 206 to accomplish it. In the system 200 of FIG. 2, each of the originators 202 and 204 has been assigned a batch job to execute, for which it does not have adequate  
5 access to resources to complete. Therefore, each of the originators 202 and 204 must ask the dispatch 201 for one or more account credentials so that it can complete its assigned job. Specifically, they request credentials of the network accounts for access to resources across the system 200 that they need to complete their jobs. Two specific cases are examined.

10 The first case involves the first originator 202. The first originator 202 – viz., such as its corresponding originating account – sends a request 208 for network account credentials that will enable the first originator 202 to complete its assigned batch job. In response, the dispatch 201 fields the request 208 and returns the credentials of its batch account, as represented by arrow 210 in FIG. 2. Thus, the batch account is “returned” as  
15 the credentials of the network account requested. The batch account credentials enable the originator 202 to complete its assigned batch job. Upon receipt of the batch account credentials, the originator 202 is able to impersonate the batch account – that is, it is able to impersonate the dispatch 201 – so that it can access resources which the batch account has permission to access.

20 The second case involves the second originator 204. The second originator 204 – viz., such as its corresponding originating account – sends a request 212 for network account credentials, again such as network account credentials that will enable the second originator 204 to complete its assigned batch job. In response, the dispatch 201 fields the



structure. In varying embodiments, the objects can be files, message queues, etc.; the invention is not so limited. The objects for the originators 202 and 204 are unpublished objects. They are not globally known, and can be accessed by other accounts that know their identities, e.g. b/c they were previously informed of their identities. It is noted that  
5 an object in one embodiment is only read-accessible by its owner.

The object for the dispatch 201 is the mechanism by which, in one embodiment, the dispatch 201 is able to receive requests such as the requests 208 and 212. Therefore, the object for the dispatch 201 is desirably a published object, so that every account within the system 200 can send a request thereto, without having to be previously  
10 informed of the object's identity. The objects for the originators 202 and 204 are the mechanisms by which, in one embodiment, the originators 202 and 204 receive account credentials satisfying their requests for network account credentials. Such requests desirably identify the objects, since they are not published, so that the dispatch 201 is able to know where to send the requested-for network account credentials.

15 In one embodiment, the network account credentials sent back to the originators 202 and 204, such as the batch account in the case of the originator 202, and the agent account in the case of the originator 204, are represented as emblems. Emblems are generally referred to herein as objects in which network account credentials can be transmitted securely, and include both the objects as well as the credentials themselves.  
20 That is, the access privileges represented by the credentials of network accounts are securely included in data that are generically referred to herein in a non-restrictive and non-limited manner as emblems. In one embodiment, the emblems are expirable, such that they are only valid for a limited period of time, to add another level of security

within the system 200. In such an embodiment, when the emblem is about to expire, it is renewed with a renewing authority – for example, the dispatch 201, although the invention is not so limited – so that the originator that is the holder of the emblem can continue to access system resources as allowed by the network access credentials encased within the emblem. The manner by which emblems are renewed is not limited by the invention. In one embodiment, the emblems are transparently renewed, while in a different embodiment, the emblems must be specifically renewed by their holders prior to expiration.

In the description of the system 200 of FIG. 2, two cases were specifically described as representative of embodiments of the invention: an originating account making a request for the credentials of a network account and receiving in response the batch account access emblem of the dispatch that includes the network account credentials for the dispatch; and, an originating account making a request for network account credentials and receiving in response the access emblem of an agent account, where the access emblem includes the network account credentials for the agent account, and where the agent was proxy logged onto by the dispatch so that its agent account could be remoted back to the originating account. It is noted, however, that each of these cases is representative of embodiments of the invention, and do not represent limitations thereon.

For example, in another embodiment, any number and any type of account can be used. Proxy logon can be used to allow network accounts to log onto other network accounts. Furthermore, any type of account can be used as the originating account, such as a local account, a machine account, or a user account. In such embodiments of the

invention, the “any number” and “any type” of account capabilities allow for any-account-to-any-account impersonation capability, as can be appreciated by those of ordinary skill within the art.

As another example, in other embodiments of the invention, the credentials requested for by the originating account can be for a type of agent account, such that any number of agent accounts have credentials satisfying the request. In such an instance, the dispatch, for example, can determine which agent account has its credentials sent back to the originating account. In other embodiments, the credentials requested for by the originating account can be for a particular agent account, such that only the credentials for this agent account can satisfy the originating account’s request.

### Methods

In this section of the detailed description, methods according to varying embodiments of the invention are described. In some embodiments, the methods are computer-implemented. The computer-implemented methods can be realized at least in part as one or more programs running on a computer – that is, as a program executed from a computer-readable medium such as a memory by a processor of a computer, such as the computer shown in and described in conjunction with FIG. 1. The programs are desirably storable on a machine-readable medium such as a floppy disk or a CD-ROM, for distribution and installation and execution on another computer.

Referring to FIG. 3, a flowchart of a method according to an embodiment of the invention is shown. In 300, a request is sent for network account credentials from an originating account to a dispatch. In one embodiment, the originating account is associated with an unpublished object, as has been described, and the dispatch is

associated with a published object, as has also been described. In such an embodiment, the request is sent to the published object, and includes identification of the unpublished object.

In 302, the dispatch authenticates the originating account. Upon authentication, a  
5 network account access emblem is sent back to the originating account as requested, where the emblem includes the credentials for a network account. In one embodiment, the access emblem of a network account is sent back to the unpublished object associated with the originating account, having the identification as initially included in the request.

This process of returning network account credentials to an originating account  
10 can be accomplished in specific embodiments by performance of 304, or by performance of 306 and 308. In 304, a batch account access emblem of the dispatch is returned to the originating account and includes its credentials. Conversely, in 306, the dispatch proxy logs onto an agent account, packs and sends its credentials to the originating account (by means of an emblem), such that in 308 the agent account access emblem is remoted to the  
15 originating account, where the emblem includes the network account credentials. It is noted that the method of FIG. 3 can be implemented in conjunction with embodiments of the invention as described in the previous section of the detailed description. Therefore, for example, the initial request sent in 300 can be unencrypted, while successive communications, such as those performed in 304, or 306 and 308, should be encrypted, as  
20 has been described. As another example, each of the published object and the unpublished object can be a message queue, a file, etc., as has been described.

Furthermore, where an emblem is sent back to the originating account, the emblem can be expirable, such that in one embodiment the method also includes determining whether

the emblem is about to expire, and upon so determining, renewing the emblem with a renewing authority, such as the dispatch, as has been described. Finally, the originating account can be one or more of a local account, a machine account, and a user account.

### Conclusion

5           Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiments shown. This application is intended to cover any adaptations or variations of the present invention. Therefore, it is manifestly intended that this invention be limited only by the  
10   claims and equivalents thereof.

We claim:

1. A computer-implemented method comprising:

    sending a request for network account credentials from an originating account  
    associated with an unpublished object to a dispatch associated with a published object,

5   the request sent to the published object associated with the dispatch includes

    identification of the unpublished object associated with the originating account;

    authenticating the originating account at the dispatch; and,

    upon authenticating the originating account, sending an emblem for a network  
    account to the originating account, the emblem sent to the unpublished object associated  
10   with the originating account and having the identification as included with the request.

2. The method of claim 1, wherein the request is unencrypted, and the emblem is  
    encrypted.

3. The method of claim 1, wherein each of the published object and the unpublished  
    object comprises a message queue.

15   4. The method of claim 1, wherein each of the published object and the unpublished  
    object comprises a file.

5. The method of claim 1, wherein the emblem comprises a token.

6. The method of claim 1, wherein the network account for which the emblem is sent from the dispatch to the originating account comprises a batch account of the dispatch.

7. The method of claim 1, wherein sending an emblem for the network account to the originating account comprises remoting the batch account to the originating account, such

5 that the emblem comprises an emblem for the batch account.

8. The method of claim 1, wherein the network account for which the emblem is sent from the dispatch to the originating account comprises an agent account of an agent.

9. The method of claim 1, wherein sending an emblem for the network account to the originating account comprises:

10 proxy logging on to the agent; and,

remoting the agent account to the originating account upon proxy log on to the agent, such that the emblem comprises an emblem for the agent account.

10. The method of claim 1, wherein the emblem is expirable, such that the method further comprises determining whether the emblem is about to expire, and upon so determining,

15 renewing the emblem with a renewing authority.

11. A computer-implemented method comprising:

sending an unencrypted request for network account credentials from an originating account to a dispatch;

authenticating the originating account at the dispatch;

upon authenticating the originating account,  
proxy logging on to an agent account; and,  
transmitting an emblem including network account credentials for one of the  
agent account and a batch account back to the originating account to satisfy the request  
5 for network account credentials sent from the originating account.

12. The method of claim 11, wherein the originating account has associated therewith an  
unpublished object, the unpublished object identified within the request from the  
originating account for credentials of a network account, and designed to receive the  
agent account emblem satisfying the request.

10 13. The method of claim 12, wherein the unpublished object comprises one of: a file, and  
a message queue.

14. The method of claim 11, wherein a published object is associated with the dispatch,  
the published object designed to receive the request for the network account credentials.

15 15. The method of claim 14, wherein the published object comprises one of: a file, and a  
message queue.

16. The method of claim 11, wherein the emblem is expirable, such that when the  
emblem is about to expire, the emblem is renewed with a renewing authority.

17. A computerized system comprising:

a plurality of network accounts, each account capable of being proxy logged onto and of being remoted to another account; and,

a dispatch designed to field requests for network account credentials from the plurality of accounts, and to satisfy each request for network account credentials from an originating account by proxy logging onto an account capable of being proxy logged onto such that credentials for the account are remoted back to the originating account as the network account credentials requested.

18. The system of claim 17, wherein the dispatch is further designed to satisfy a request for network account credentials from an originating account by returning an emblem including network account credentials for a batch account of the dispatch as the network account credentials requested.

19. The system of claim 17, wherein the dispatch is further designed to satisfy a request for network account credentials from an originating account only upon first authenticating the originating account.

20. The system of claim 17, wherein a published object is associated with the dispatch, the published object designed to receive the requests for network account credentials.

21. The system of claim 20, wherein the published object comprises one of: a file, and a message queue.

## ABSTRACT OF THE DISCLOSURE

The invention relates to secured distributed impersonation, for use within systems such as batch system and batch message transaction systems. In one embodiment, a method includes sending a request for credentials of a network account from an

5 originating account associated with an unpublished object to a dispatch associated with a published object. In one embodiment, both the unpublished and the published objects can each be a message queue. The dispatch authenticates the originating account. Upon successful authentication, the network account access emblem is sent to the originating account – that is, the originating account receives the requested credentials, which

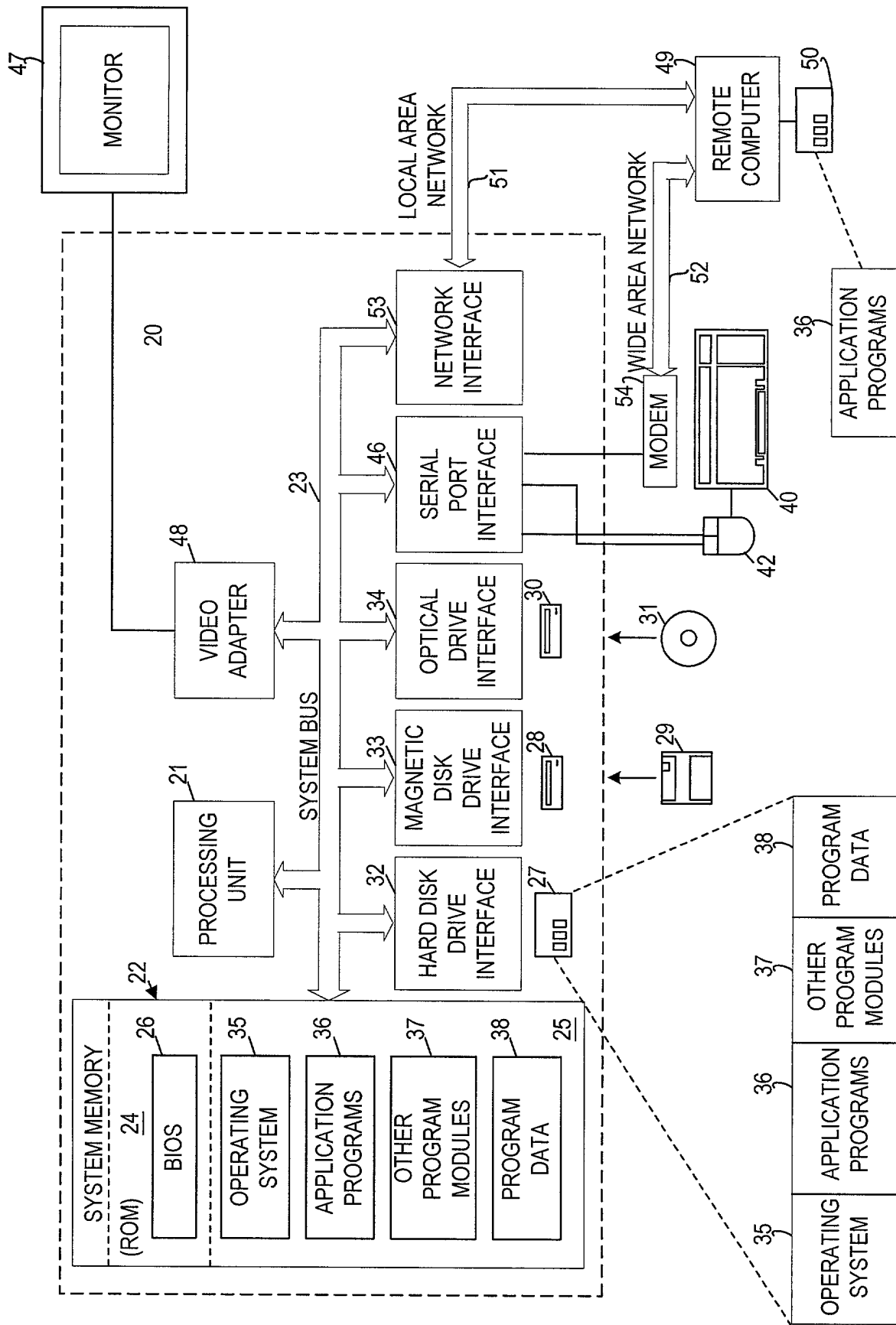
10 facilitate the ability to impersonate into the network account.

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to addressee" service under 37 CFR § 1.10 in an envelope addressed to The Assistant Commissioner for Patents, Washington, DC 20231, on Mar 1, 2000, by Michael Dryja, and having "express mail" mailing label no. EK530297201US.



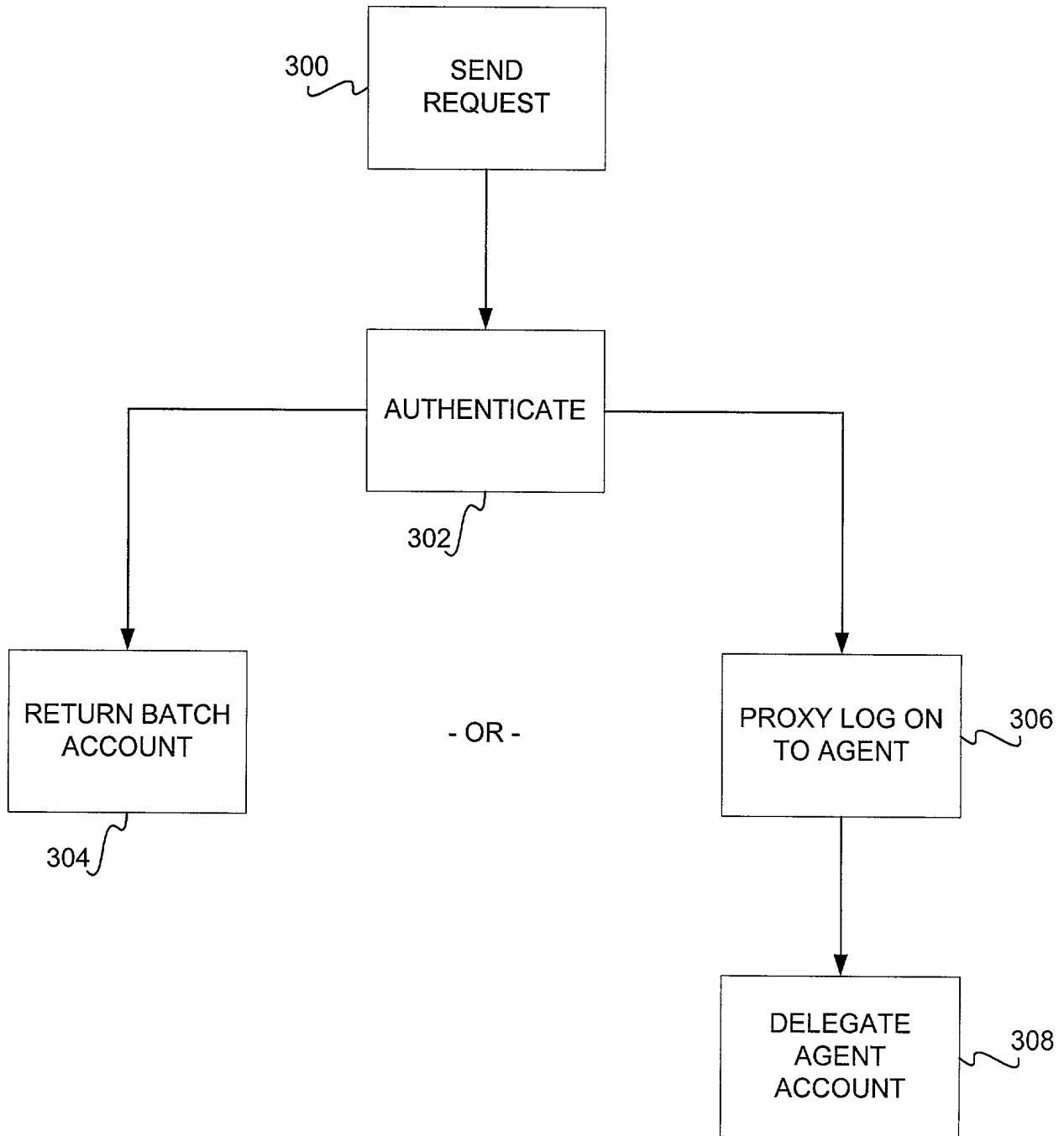
Signature of Michael Dryja

FIG. 1





**FIG 3**



# PATENT APPLICATION

## DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

ATTORNEY DOCKET NO. 1018.072US1

As a below named inventor, I hereby declare that:

My residence/post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Secured Distributed Impersonation

the specification of which is attached hereto unless the following box is checked:

( ) was filed on \_\_\_\_\_ as US Application Serial No. or PCT International Application  
Number \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable).

I hereby state that I have reviewed and understood the contents of the above-identified specification, including the claims, as amended by any amendment(s) referred to above. I acknowledge the duty to disclose all information which is material to patentability as defined in 37 CFR 1.56.

### Foreign Application(s) and/or Claim of Foreign Priority

I hereby claim foreign priority benefits under Title 35, United States Code Section 119 of any foreign application(s) for patent or inventor(s) certificate listed below and have also identified below any foreign application for patent or inventor(s) certificate having a filing date before that of the application on which priority is claimed:

COUNTRY	APPLICATION NUMBER	DATE FILED	PRIORITY CLAIMED UNDER 35 U.S.C. 119
			YES: ____ NO: ____
			YES: ____ NO: ____

### Provisional Application

I hereby claim the benefit under Title 35, United States Code Section 119(e) of any United States provisional application(s) listed below:

APPLICATION SERIAL NUMBER	FILING DATE

### U.S. Priority Claim

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code Section 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, Section 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

APPLICATION SERIAL NUMBER	FILING DATE	STATUS(patented/pending/abandoned)

### POWER OF ATTORNEY:

As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) listed below to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

**Michael A. Dryja, Reg. No. 39662**

**Katie E. Sako, Reg. No. 32628**

**Daniel D. Crouse, Reg. No. 32022**

### Send Correspondence to:

**Michael A. Dryja**  
**Law Offices of Michael Dryja**  
**704 228th Avenue NE**  
**PMB 694**  
**Redmond, WA 98053**

### Direct Telephone Calls To:

**Michael A. Dryja**  
**425-427-5094**

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**Full Name of Inventor: Neta Amit**

**Citizenship: Israeli**

**Residence: 33 Yotam Street, Haifa, 34675 Israel**

**Post Office Address: Same**

\_\_\_\_\_  
Inventor's Signature

\_\_\_\_\_  
Date

DECLARATION AND POWER OF ATTORNEY  
FOR PATENT APPLICATION (continued) ATTORNEY DOCKET NO. 1018.072US1

DECLARATION AND POWER OF ATTORNEY  
FOR PATENT APPLICATION (continued) ATTORNEY DOCKET NO. 1018.072US1

**Citizenship:** Israeli, German

**Residence:** 11 Mizpe St., Ramat-Gan, 52493 Israel

**Post Office Address: Same**

**Inventor's Signature**

Date \_\_\_\_\_

I hereby certify that this is being deposited with the United States Postal Service "Express Mail Post Office to addressee" service under 37 CFR § 1.10 in an envelope addressed to The Assistant Commissioner for Patents, Washington, DC 20231, on Mar 1, 2000, by Michael Dryja, and having "express mail" mailing label no. EK530297201US.

One way

Signature of Michael Dryja

22042  
 22043  
 22044  
 22045  
 22046  
 22047  
 22048  
 22049  
 22050  
 22051  
 22052  
 22053  
 22054  
 22055  
 22056  
 22057  
 22058  
 22059  
 22060  
 22061  
 22062  
 22063  
 22064  
 22065  
 22066  
 22067  
 22068  
 22069  
 22070  
 22071  
 22072  
 22073  
 22074  
 22075  
 22076  
 22077  
 22078  
 22079  
 22080  
 22081  
 22082  
 22083  
 22084  
 22085  
 22086  
 22087  
 22088  
 22089  
 22090  
 22091  
 22092  
 22093  
 22094  
 22095  
 22096  
 22097  
 22098  
 22099  
 22100  
 22101  
 22102  
 22103  
 22104  
 22105  
 22106  
 22107  
 22108  
 22109  
 22110  
 22111  
 22112  
 22113  
 22114  
 22115  
 22116  
 22117  
 22118  
 22119  
 22120  
 22121  
 22122  
 22123  
 22124  
 22125  
 22126  
 22127  
 22128  
 22129  
 22130  
 22131  
 22132  
 22133  
 22134  
 22135  
 22136  
 22137  
 22138  
 22139  
 22140  
 22141  
 22142  
 22143  
 22144  
 22145  
 22146  
 22147  
 22148  
 22149  
 22150  
 22151  
 22152  
 22153  
 22154  
 22155  
 22156  
 22157  
 22158  
 22159  
 22160  
 22161  
 22162  
 22163  
 22164  
 22165  
 22166  
 22167  
 22168  
 22169  
 22170  
 22171  
 22172  
 22173  
 22174  
 22175  
 22176  
 22177  
 22178  
 22179  
 22180  
 22181  
 22182  
 22183  
 22184  
 22185  
 22186  
 22187  
 22188  
 22189  
 22190  
 22191  
 22192  
 22193  
 22194  
 22195  
 22196  
 22197  
 22198  
 22199  
 22200  
 22201  
 22202  
 22203  
 22204  
 22205  
 22206  
 22207  
 22208  
 22209  
 22210  
 22211  
 22212  
 22213  
 22214  
 22215  
 22216  
 22217  
 22218  
 22219  
 22220  
 22221  
 22222  
 22223  
 22224  
 22225  
 22226  
 22227  
 22228  
 22229  
 22230  
 22231  
 22232  
 22233  
 22234  
 22235  
 22236  
 22237  
 22238  
 22239  
 22240  
 22241  
 22242  
 22243  
 22244  
 22245  
 22246  
 22247  
 22248  
 22249  
 22250  
 22251  
 22252  
 22253  
 22254  
 22255  
 22256  
 22257  
 22258  
 22259  
 22260  
 22261  
 22262  
 22263  
 22264  
 22265  
 22266  
 22267  
 22268  
 22269  
 22270  
 22271  
 22272  
 22273  
 22274  
 22275  
 22276  
 22277  
 22278  
 22279  
 22280  
 22281  
 22282  
 22283  
 22284  
 22285  
 22286  
 22287  
 22288  
 22289  
 22290  
 22291  
 22292  
 22293  
 22294  
 22295  
 22296  
 22297  
 22298  
 22299  
 22300  
 22301  
 22302  
 22303  
 22304  
 22305  
 22306  
 22307  
 22308  
 22309  
 22310  
 22311  
 22312  
 22313  
 22314  
 22315  
 22316  
 22317  
 22318  
 22319  
 22320  
 22321  
 22322  
 22323  
 22324  
 22325  
 22326  
 22327  
 22328  
 22329  
 22330  
 22331  
 22332  
 22333  
 22334  
 22335  
 22336  
 22337  
 22338  
 22339  
 22340  
 22341  
 22342  
 22343  
 22344  
 22345  
 22346  
 22347  
 22348  
 22349  
 22350  
 22351  
 22352  
 22353  
 22354  
 22355  
 22356  
 22357  
 22358  
 22359  
 22360  
 22361  
 22362  
 22363  
 22364  
 22365  
 22366  
 22367  
 22368  
 22369  
 22370  
 22371  
 22372  
 22373  
 22374  
 22375  
 22376  
 22377  
 22378  
 22379  
 22380  
 22381  
 22382  
 22383  
 22384  
 22385  
 22386  
 22387  
 22388  
 22389  
 22390  
 22391  
 22392  
 22393  
 22394  
 22395  
 22396  
 22397  
 22398  
 22399  
 22400  
 22401  
 22402  
 22403  
 22404  
 22405  
 22406  
 22407  
 22408  
 22409  
 22410  
 22411  
 22412  
 22413  
 22414  
 22415  
 22416  
 22417  
 22418  
 22419  
 22420  
 22421  
 22422  
 22423  
 22424  
 22425  
 22426  
 22427  
 22428  
 22429  
 22430  
 22431  
 22432  
 22433  
 22434  
 22435  
 22436  
 22437  
 22438  
 22439  
 22440  
 22441  
 22442  
 22443  
 22444  
 22445  
 22446  
 22447  
 22448  
 22449  
 22450  
 2